

Exhibit # 1

UNITED STATES DISTRICT COURT

for the
Western District of Michigan

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

1733 OWASIPPE ROAD
TWIN LAKE, MICHIGAN 49457

Case No. 1:10-MJ-344

Certified as a True Copy
By M. Hetherington
Deputy Clerk
U. S. District Court
Western Dist. of Michigan
Date JUL 1 2010

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Western District of Michigan, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2252A(a)(1)	Transmission, receipt, and possession of child pornography
18 USC 2252A(a)(2)	
18 USC 2252A(a)(5)(B)	

The application is based on these facts:

See

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/

Applicant's signature

Adam J. Van Deuren, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 07/01/2010

JOSEPH G. SCOVILLE

Judge's signature

City and state: Grand Rapids, Michigan

Joseph G. Scoville, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN

IN THE MATTER OF A SEARCH OF
1733 OWASIPPE ROAD,
TWIN LAKE, MICHIGAN, 49457

AFFIDAVIT

I, Adam J. Van Deuren, being duly sworn, depose and say that:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed since April 2005. I am currently assigned to the Grand Rapids Resident Agency, Grand Rapids, Michigan. In my employment as an FBI SA, I have investigated various types of Federal criminal violations, including but not limited to computer crimes, sexual exploitation of children, and child pornography matters.
2. This affidavit is being submitted in support of an Application for a Search Warrant to search for and seize the Internet router and all computers possessed by Gerber Boy Scout Camp and camp employees and staff members located at **1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457** for evidence of violations of Title 18, United States Code, § 2252A(a)(1), concerning the transmission of child pornography in interstate commerce, and Title 18, United States Code, § 2252A(a)(2), concerning the receipt or distribution of child pornography, Title 18, United States Code, § 2252A(a)(5)(B), concerning the possession of child pornography, and/or Title 18 Section 2252A(a)(3)(B) concerning promoting and presenting child pornography in interstate and foreign commerce by means of a computer.
3. The location to be searched is the Gerber Boy Scouts Camp located at **1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457**. Gerber Boy Scout Camp consists of the "Gerber Boy Scout Camp" and the "Cub Scout and Webelos Adventureland." It is a multi-acre facility south of Owasisippe Road and

west of Blue Lake Road in Muskegon County. The Camp has multiple permanent structures, including offices and housing for staff and employees. Based upon the information summarized here, I have reason to believe that evidence of violations of the Federal criminal statutes noted in paragraph 2 is within the router(s) located at this premises.

- JS*
4. *computers and* The factual basis set forth in this affidavit in support of the application for the search warrant is based upon information I discovered in the course of my investigation, information from other FBI Special Agents, FBI computer forensic examiners, other law enforcement officers or agencies, public records, and information from Internet Service Providers obtained during this investigation. The factual basis also includes information based on my own experience in and knowledge of computer crimes and child pornography investigations as well as the experience, knowledge and expertise of other investigators and forensics examiners. Not all of the information I have acquired in this investigation is contained within this affidavit.

Child Pornography and Peer-To-Peer Technology

5. Computers and the Internet are regularly used in the production, distribution, trading, and possession of child pornography. One method used in the distribution and trade of child pornography on the Internet is peer-to-peer (hereinafter referred to as P2P) file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. There are several P2P networks and software applications currently operating. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by accessing the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

6. One of the newest evolutions of P2P software allows users to set up their own private P2P network of contacts. File sharing through this new and publicly available P2P file sharing program is limited to only other users who have been added to your private list of "friends." A new user is added to your list of friends through a friend request. Acceptance of a friend request will allow that new user to download file(s) from the user who sent the friend request. The new user can then browse the list of files the other user has available to download, select the file(s) from this list, and download the selected file(s). The download of a file is achieved through a direct, encrypted connection between the computer requesting the file and the computer containing the file. This new P2P file sharing program affords those trafficking in child pornography greater control or discretion regarding the individuals with whom they share and a more secure mechanism to engage in illegal activity through the use of encrypted transfers. This new P2P file sharing program must present on a computer to be utilized.
7. Internet Protocol (IP) addresses are expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address resolves to a unique location, making it possible for data to be transferred between specific computers. Software is available to identify the IP address of the P2P computer sending the file.
8. Internet Service Providers (ISPs) assign IP addresses to their subscribers for use while accessing the Internet. These records are retrievable, allowing the subscriber whose account was used during an Internet session to be identified. In many cases, these Internet sessions can also be traced to a physical location.
9. The computers that are linked together to form the P2P network are located throughout the world and operate in interstate and foreign commerce. A person who includes child pornography files in his/her "shared" folder is hosting child pornography and is promoting, presenting, and potentially distributing child pornography. A person who hosts child pornography is in violation of Title 18 Section 2252A(a)(3)(B) in that he/she is promoting and presenting child pornography in interstate commerce by means of a computer.

Factual Basis

10. On April 24, 2010, Special Agent (SA) Barry Couch of the Federal Bureau of Investigation (FBI) office in Rochester, New York, working in an undercover capacity, used an undercover account to access a private P2P network. SA Couch queried his network of "friends" who had previously invited SA Couch's undercover persona to trade files within a private network. SA Couch identified a "friend" within the private network using the username "**Joshiex**," who was also logged into the network during SA Couch's undercover session.
11. SA Couch established a peer-to-peer connection with "**Joshiex**" and browsed the directories being made available for sharing by "**Joshiex**." SA Couch accessed the shared directories and observed many video and image files with file names indicative of child pornography. SA Couch then selected and downloaded multiple video files that depict child pornography.
12. After downloading the files, SA Couch determined that they contained child pornography. A selection of the downloaded files are identified by name and described below. Copies of the images identified below are provided in Exhibit A.
 - a. anal.mpg

This video file depicts an adult male performing anal sex on a young prepubescent male child.
 - b. FyouMultiply - 7 YO Boy.wmv

This video file depicts an adult male performing anal sex on a young prepubescent male child.

c. Hedone's Site - hotondad2.mpeg

This video file depicts an adult male performing anal sex on a young prepubescent male child.

d. Logan0.wmv

This image depicts an adult male performing oral sex on a young prepubescent male child.

e. P101 - Brotherlove 1.divx

This video file depicts multiple nude prepubescent male children lewdly and lasciviously displaying their genitalia for the camera.

13. During the download, SA Couch identified the IP address utilized by "**Joshiex**", which was **67.208.238.110**. SA Couch identified and served a subpoena on the Internet Service Provider (ISP), AriaLink. AriaLink is a small local ISP operating in West Michigan. A representative AriaLink contacted SA Couch on May 13, 2010 and advised that AriaLink did not maintain any IP information.
14. On June 17, 2010, SA Couch, working in an undercover capacity in Rochester, NY, used an undercover account to access a private P2P network. SA Couch again established an undercover session with user "**Joshiex**".
15. SA Couch used the browse function to review the files being made available for sharing by "**Joshiex**." SA Couch accessed the shared directories and observed approximately 436 video and image files with file names indicative of child pornography that were available to be shared. SA Couch then selected and downloaded approximately 12 video files that appeared to depict child pornography.

16. After downloading the files, it was determined that 12 video files appeared to be child pornography. One additional inconclusive video was also downloaded. A selection of the downloaded files are identified by name and described below. Copies of the images identified below are provided in Exhibit B.

- a. 02.avi
An adult male engaging in anal sex with a prepubescent male.
- b. 2BoyzMaknLove02[1][2].mpeg
Two prepubescent males engaging in oral sex.
- c. 13 yo boy jerks off and cums in bedroom 3'59.mpg
A prepubescent male masturbating.
- d. Hedone's Site - hotondad2.mpeg
An adult male engaging in anal sex with a prepubescent male.
- e. little boy sucks and gets cum in his mouth.mpg
Two prepubescent males engaging in oral sex.

17. During the download, SA Couch identified the IP address utilized by "Joshiex", which was **67.208.225.149**. SA Couch again served a subpoena to AriaLink which advised that it had begun maintaining IP address log information. SA Couch obtained IP records from AriaLink on approximately June 17, 2010 as to the user assigned IP Address **67.208.225.149** on June 17, 2010, at the time of the downloads from "Joshiex." These records indicated that the user assigned the IP address was on the account of Scott Herrick, **1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457**. Additionally, AriaLink provided the subscriber's telephone number as **231-894-4928** ext. 000 and the subscriber's email address as gerberscoutcamp@gmail.com.

18. At the time of the aforementioned downloads from "**Joshiex**," SA Couch was physically located in the State of New York.
19. On June 30, 2010, I obtained information that Scott Herrick is the Camp Director for the Gerber Boy Scout Camp in Twin Lake, Michigan. Additionally, I was advised that the Gerber Boy Scout camp was not yet open to campers on April 24, 2010 and would have only been occupied by camp staff members.
20. I conducted a public records search of the telephone number **231-894-4928** and discovered that the number is subscribed to The Boy Scouts of America, **1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457.**
21. On June 29, 2010, I was contacted by SA Thomas Thompson from the FBI office in New York, NY. SA Thompson advised that he had conducted an online undercover session with "**Joshiex**" on June 25, 2010 at approximately 10:49 AM and viewed multiple images and videos of child pornography that were available by "**Joshiex**" for download. SA Thompson advised that the IP address used by "**Joshiex**" belongs to AriaLink and served a subpoena to them, however he has not yet received a subpoena return with subscriber information.
22. SA Thompson further advised that within the shared folder were images of teenaged boys in Boy Scout uniforms. One of the images depicted a child in a Boy Scout uniform with his genitals exposed. SA Thompson is experienced in investigating child pornography cases and described the image as "child pornography."
23. AriaLink advised that the Internet account service remained active as of June 30, 2010, and is subscribed to by the same customer as at the time of the transfer of child pornography to an FBI undercover agent. AriaLink further advised that the camp uses a router for Internet service, which permits multiple computers to access the Internet.

Considerations Relating to this Investigation

24. In a wireless or wired computer network, a router is used to control and maintain Internet access for multiple computers. Each computer has a unique identifying number, called a MAC address, and the router will identify and log the MAC address(es) of the computers accessing the Internet. It may be possible to identify the individual computer that contains the specialized P2P software and the child pornography collection by comparing the Internet log activity from the router with the date and time of the undercover connections. MAC addresses for laptop computers are printed on the exterior of the computer. Reviewing the MAC addresses will require seizing the computers.
25. It is also possible to identify the computer that contains the specialized P2P software and child pornography collection by turning on the computer and browsing the software program files. If present, the P2P program will be listed.
26. Once the computer that contains the specialized P2P software is identified it will be subject to a complete examination by a computer forensic examiner.
27. Digital evidence of different types can be recovered from the hard drives of computers depending on a variety of factors, among which is the skill and ability of the user to clean or hide such evidence on the computer. Saved files, temporary files, and even deleted files of all types can be recovered from a computer by a trained forensic examiner. In certain circumstances, password protected and encrypted files may be recoverable by a trained forensic examiner.
28. The computer may provide information about the source of child pornography images on the Internet, other individuals involved in the collection, trafficking and trade of child pornography, the identification of child victims and, possibly, of related crimes including the enticement of minors for sexual purposes or the production of child pornography. Therefore, this warrant seeks permission to seize the computer and to search it for evidence in the form of child pornography images or videos, stored e-mails associated with the receipt and distribution of such images, and any chat or other text files relating to contact with collectors of child pornography or with actual children. In conducting the search, the forensic

examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches which may result in the display of irrelevant materials.

29. Individuals interested in child pornography will often produce or attempt to produce child pornography by taking their own pictures and videos.
30. The Government requests permission to secure the computer to have it examined in a controlled environment utilizing specialized software and hardware. This insures the safety of evidence and the property itself from unintended destruction or damage and minimizes the possibility of evidence being intentionally destroyed.
31. Because of the nature and complexity inherent in computer searches, the time period required for a complete, safe, and secure forensic examination of the computer hard drive and storage media is uncertain. Upon determining the extent of material seized requiring forensic examination and any special forensic examination requirements, the Government will provide the Court an estimate of the time required to complete the forensic examinations along with the search warrant return.
32. It is further noted that retention of any computers would be warranted, should any child pornography be found thereon, in order to permit forfeiture of those computers and related properties as instrumentalities of the crime, pursuant to Title 18, United States Code, § 2253(a)(3), or Title 18, United States Code, § 2254(a)(2).

Conclusion

33. The evidence obtained and developed in this investigation has shown the existence of specialized P2P software and a collection of child pornography on a computer connected to the AriaLink Internet service physically located at the Gerber Boy Scout Camp, 1733 OWASIPPE ROAD, TWIN LAKE,

MICHIGAN, 49457. The investigation also identified that this collection of child pornography was being offered for downloading to others using a private P2P network and that the private network included others outside the State of Michigan via the Internet. The investigation also shows evidence of an interstate electronic transfer of multiple images of child pornography to two undercover FBI agents, the images being received from a computer connected to the Internet service physically located at the residence at **1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457.**

34. Based upon the fact that the first session occurred before any campers were present, it is probable that the person using the computer is an employee or staff member. I am seeking permission to seize all computers (including desktop and laptop computers) possessed by Gerber Boy Scout Camp and all employees and staff members of the Boy Scout Camp and within the premises at the time of the execution of this warrant. I will seek the assistance of the staff members to locate and secure all the staff members' computers to avoid conducting a physical search of the entire camp. One or more computer forensic examiner will be on scene and will attempt to identify the computer through the router. If unsuccessful, we will conduct a limited examination of the computers only to determine which computer contains the specialized P2P software. Once that computer is located, I am seeking permission to then conduct a full computer forensic examination of the contents of that computer, including but not limited to an inventory of the images, evidence of the production, distribution and possession of child pornography. I am also seeking permission to seize and search any camera that is possessed by the owner of the computer that contains the specialized P2P software.

35. Based on information outlined above, as well as my knowledge and experience relating to child pornography investigations, and the knowledge and experience of others in child pornography investigations and forensic examinations, I have probable cause to believe that evidence will be found at **1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457,** including the following:


- a. The router that provides the connection to the ISP and the Internet service. Within that

router will be information identifying all computers that were utilizing that connection.

- b. The computer that contains the specialized peer-to-peer software and the child pornography collection.
- c. A digital camera or other digital imaging device.

36. WHEREFORE, based on the facts set forth above, your Affiant submits there is probable cause to believe that evidence of the receipt, possession, or transmission of child pornography, in violation of 18 U.S.C. 2252A, exists on or within computers or other digital storage media located at **1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457,**

37. Your Affiant respectfully requests that the Court issue a warrant to search for and seize the items listed in Attachment B and located at Gerber Boy Scout Camp at **1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457.**


ADAM J. VAN DEUREN
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 1st day of July, 2010.

JOSEPH G. SCOVILLE

HON. JOSEPH G. SCOVILLE
United States Magistrate Judge
Western District of Michigan

ATTACHMENT A

Gerber Boy Scouts Camp is located at 1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457. Gerber Boy Scout Camp consists of the “Gerber Boy Scout Camp” and the “Cub Scout and Webelos Adventureland.” It is a multi-acre facility south of Owasppe Road and west of Blue Lake Road in Muskegon County. The Camp has multiple permanent structures, including offices and housing for staff and employees.

ATTACHMENT B

Items to be seized and searched:

1. The router that provides the connection to the ISP and Internet service.
2. All computers (including desktop and laptop computers) possessed by the Gerber Boy Scout Camp and all employees and staff members of the Boy Scout Camp and within the premises at the time of the execution of this warrant. Staff members will be asked to assist in locating and securing all the staff members' computers to avoid conducting a physical search of the entire camp. One or more computer forensic examiner will be on scene and will attempt to identify the particular computer that contains the specialized peer-to-peer software and the child pornography collection by the MAC address. If unsuccessful, the computer forensic examiner will conduct a limited examination of the computers only to determine which computer contains the specialized peer-to-peer software. Once that computer is located, the computer forensic examiner will conduct a full computer forensic examination of the contents of that computer, including but not limited to an inventory of the images, evidence of the production, distribution and possession of child pornography.
3. Digital camera(s) or other digital imaging device(s) possessed by the owner of the computer that contains the specialized peer-to-peer software.

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Michigan

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))

1733 OWASIPPE ROAD)
 TWIN LAKE, MICHIGAN 49457)

Case No. 1:10-MJ-344

SEARCH AND SEIZURE WARRANT

Certified as a True Copy
 By M. Hittington
 Deputy Clerk
 U.S. District Court
 Western Dist. of Michigan
 Date JUL 1 2010

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Michigan
 (identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

JUL 15 2010

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Joseph G. Scoville
 (name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for days (not to exceed 30).

☐ until, the facts justifying, the later specific date of .

Date and time issued:

JUL 1 2010JOSEPH G. SCOVILLE

Judge's signature

City and state: Grand Rapids, MichiganJoseph G. Scoville, U.S. Magistrate Judge

Printed name and title

Return		
Case No.: 1:10-MJ-344	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: _____	<div style="text-align: center;"> _____ <i>Executing officer's signature</i> </div>	
	<div style="text-align: center;"> _____ <i>Printed name and title</i> </div>	

ATTACHMENT A

Gerber Boy Scouts Camp is located at 1733 OWASIPPE ROAD, TWIN LAKE, MICHIGAN, 49457. Gerber Boy Scout Camp consists of the "Gerber Boy Scout Camp" and the "Cub Scout and Webelos Adventureland." It is a multi-acre facility south of Owasippe Road and west of Blue Lake Road in Muskegon County. The Camp has multiple permanent structures, including offices and housing for staff and employees.

ATTACHMENT B

Items to be seized and searched:

1. The router that provides the connection to the ISP and Internet service.
2. All computers (including desktop and laptop computers) possessed by the Gerber Boy Scout Camp and all employees and staff members of the Boy Scout Camp and within the premises at the time of the execution of this warrant. Staff members will be asked to assist in locating and securing all the staff members' computers to avoid conducting a physical search of the entire camp. One or more computer forensic examiner will be on scene and will attempt to identify the particular computer that contains the specialized peer-to-peer software and the child pornography collection by the MAC address. If unsuccessful, the computer forensic examiner will conduct a limited examination of the computers only to determine which computer contains the specialized peer-to-peer software. Once that computer is located, the computer forensic examiner will conduct a full computer forensic examination of the contents of that computer, including but not limited to an inventory of the images, evidence of the production, distribution and possession of child pornography.
3. Digital camera(s) or other digital imaging device(s) possessed by the owner of the computer that contains the specialized peer-to-peer software.